

日本国特許庁
JAPAN PATENT OFFICE

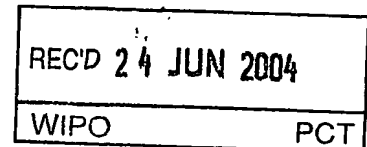
23.04.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 3月17日

出願番号
Application Number: 特願2003-072372
[ST. 10/C]: [JP 2003-072372]



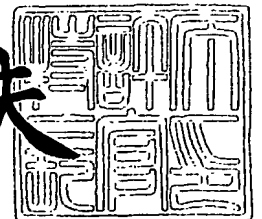
出願人
Applicant(s): セイコーエプソン株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 6月 2日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 J0096564

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/00

【発明者】

【住所又は居所】 長野県諏訪市大和 3 丁目 3 番 5 号 セイコーエプソン株式会社内

【氏名】 黒田 直人

【特許出願人】

【識別番号】 000002369

【氏名又は名称】 セイコーエプソン株式会社

【代理人】

【識別番号】 100095728

【弁理士】

【氏名又は名称】 上柳 雅誉

【連絡先】 0 2 6 6 - 5 2 - 3 1 3 9

【選任した代理人】

【識別番号】 100107076

【弁理士】

【氏名又は名称】 藤網 英吉

【選任した代理人】

【識別番号】 100107261

【弁理士】

【氏名又は名称】 須澤 修

【手数料の表示】

【予納台帳番号】 013044

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0109826

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラム

【特許請求の範囲】

【請求項 1】 ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 2】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 3】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、

当該プログラムの起動時の、ネット接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 4】 コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する、制御プログラムを、

自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 5】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【請求項 6】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【請求項 7】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 8】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムによる、ネット接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 9】 請求項 1 に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項 10】 ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

【請求項 11】 コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

前記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ウィルス対策ソフトによる定義ファイルの修正分取り込み処理等の制御により、ネットワーク接続時のセキュリティを高めたネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラムに関する。

【0002】

【従来の技術】

コンピュータウィルスに対する対策のためにコンピュータにインストールされた対策ソフトは、通常、コンピュータを起動したときに立ち上がる。そして、コンピュータをネットワークに接続すると、一定時間おきにネットワークを通じて所定のサーバに接続し、ウィルス対策用定義ファイルの定義ファイルの修正分取り込み処理をする。即ち、定義ファイルのバージョンが変わっている場合には、差分を取り込んだり、更新されたファイル全体を取り込むことにより、定義ファイルを更新する。その後は、同様の処理を自動的に周期的に繰り返す。こうしたワクチンやパターンファイルの更新技術が紹介されている（特許文献1参照）。

【特許文献1】 特開2002-259150号公報

【0003】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

モバイルコンピュータは、ネットワークに接続される前に起動して、ローカルで使用されることが多い。ウィルス対策ソフトはモバイルコンピュータの起動と同時に起動して、周期的に定義ファイルの修正分取り込み処理を試みるが、ネットワークに接続されていないから、ファイルの更新に失敗する。場合によっては

、長期間定義ファイルの修正分取り込み処理がなされないままになっていることもある。こうしたコンピュータを起動させたままの状態、突然ネットワークに接続すると、ウィルス対策ソフトが次のタイミングで定義ファイルの修正分取り込み処理を実行するまでは、新種のウィルスに対し、無防備な状態になる。

本発明は、以上の点に着目してなされたもので、通信を実行するプログラムの起動時に、自動的にセキュリティ対策用ファイルの更新処理を実行させるようにしたネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラムを提供することを目的とする。

【0004】

【課題を解決するための手段】

本発明は次の構成により上記の課題を解決する。

〈構成1〉

ネットワークに接続をして通信を実行するプログラムの起動時に、上記ネットワークへの接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0005】

セキュリティ対策用ファイルの更新処理とは、ウィルス対策用の定義ファイルの修正分取り込み処理や、パッチファイルの取り込み処理のように、コンピュータをネットワークに接続した場合のセキュリティ対策用ファイルを、ネットワークを通じて取得して更新する処理のことである。修正分は、差分データのこともあるし、修正して更新されたデータファイルのこともある。この処理は、ネットワークに接続をして通信を実行するプログラムの起動時に実行される。ネット接続処理後他の処理に先行するから、通信を実行するプログラムの動作開始前に最新のセキュリティ対策が施される。ネットワークへの接続が長時間に及ぶ場合は、その後一定時間おきにセキュリティ対策用ファイルの更新処理を起動することが好ましい。

【0006】

〈構成2〉

構成 1 に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0007】

セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力することで、利用者は、安心してネットワークを利用できる。また、動作エラーにより無防備な状態になったときは、ネットワークを切断する等の処置ができる。

【0008】

〈構成 3〉

構成 1 に記載のネットワークセキュリティ強化システムにおいて、既に起動しているコンピュータであって、ネットワークに未接続の状態、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、当該プログラムの起動時の、ネット接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0009】

ネットワーク接続後はウィルス対策プログラムが定期的に動作するから、その後通信を実行するプログラムの再立ち上げや追加立ち上げをしても、セキュリティ対策用ファイルの更新処理をさせない。これにより、通信を実行するプログラムの立ち上げ処理が速くなる。

【0010】

〈構成 4〉

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する、制御プログラムを、自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0011】

上記の構成のシステムを実現するには、ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動するという制御プログラムが必要である。しかしながら、コンピュータによって、インストールされている通信用のプログラムが異なる。そこで、あらかじめ、コンピュータにインストールされた、通信用のプログラムを検出し、自動的に制御プログラムを生成する手段を設けた。これにより、各種の通信用プログラムをインストールした任意のコンピュータに対して、上記の機能を容易に付与できる。

【0012】**〈構成5〉**

構成1に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【0013】

セキュリティ対策として最も重要な処理である。

【0014】**〈構成6〉**

構成1に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【0015】

セキュリティホール対策として、パッチファイルの取り込みを先行させることも重要である。

【0016】**〈構成7〉**

構成1に記載のネットワークセキュリティ強化システムにおいて、ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0017】

ブラウザを立ち上げる場合には、始めに定義ファイルの修正分取り込み処理を行い、その後ブラウザの画面表示を実行する。ブラウザの画面表示をしたときには、既にネットワークからウイルスが侵入するおそれがあるからである。

【0018】

〈構成8〉

構成1に記載のネットワークセキュリティ強化システムにおいて、ネットワークに接続をして通信を実行するプログラムによる、ネット接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0019】

メールソフトやブラウザやダイヤルアッププログラムなどの立ち上げ時の画面に、定義ファイルの更新をして下さい、というメッセージが表示出力される。メッセージは音声で出力されても構わない。セキュリティ対策用ファイルの更新処理は、通信を実行するプログラムと連動していなくて構わない。この場合には、無用なファイル更新処理を回避することができる。

【0020】

〈構成9〉

構成1に記載のネットワークセキュリティ強化システムにおいて、ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【0021】

ブラウザの起動時に、定義ファイルやパッチファイルの更新をして下さい、というメッセージが表示出力される。従って、自動化はされないが、セキュリティは確保される。

【0022】

〈構成10〉

ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

【0023】

構成1のシステムを実現するためのコンピュータプログラムの発明である。

【0024】

〈構成11〉

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、上記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。

【0025】

構成4の制御プログラムを自動的に生成するプログラムの発明である。

【0026】

【発明の実施の形態】

以下、本発明の実施の形態を、具体例を用いて説明する。

図1は、ネットワークセキュリティ強化システムの具体例を示すブロック図である。

図のように、セキュリティ強化の対象になっているコンピュータ10は、ネットワークインタフェース11を介してネットワーク1に接続されている。コンピュータ10には、記憶装置12と演算処理装置が設けられている。演算処理装置は、メーラー（メール管理プログラム）13とブラウザ14とダイヤルアッププログラム15とウィルス対策プログラム16とネット接続制御プログラム17から構成される。ウィルス対策プログラム16は、定義ファイル修正分取り込みプログラム18を備える。これらの演算処理装置は、コンピュータ10を動作させるコンピュータプログラムからなる。ネットワーク1にはウィルス対策プログラムの提供元のサーバ20が接続されている。このサーバ20には記憶装置21が

設けられており、定義ファイル 22 を、ネットワーク 1 を通じてユーザに提供するようになっている。

【0027】

メーラー（メール管理プログラム）13 は、メールの送受信を制御するプログラムである。ブラウザ 14 は、インターネット閲覧用のプログラムである。ダイヤルアッププログラム 15 は、あらかじめ設定された電話番号に対してダイヤルアップ接続をする制御を行うプログラムである。ウィルス対策プログラム 16 は、ウィルスチェックを実行するプログラムである。ウィルス対策プログラム 16 が動作するためには定義ファイル 22 が必要になる。ウィルス対策プログラム 16 の提供元は、新たなウィルスが発生するたびに定義ファイル 22 の修正分ファイルを提供する。ウィルス対策プログラム 16 は、あらかじめ設定された時間間隔で周期的に定義ファイル修正分取り込みプログラム 18 を起動する。定義ファイル修正分取り込みプログラム 18 は、所定のタイミングで定期的にサーバ 20 から定義ファイル 22 をダウンロードし記憶装置 12 に記憶させる機能を持つ。

【0028】

ネット接続制御プログラム 17 は、メーラー（メール管理プログラム）13 やブラウザ 14 を利用するために、ユーザがいずれかを起動すると、まず、ダイヤルアッププログラム 15 を起動し、次にウィルス対策プログラム 16 の定義ファイル修正分取り込みプログラム 18 を起動する。こうして、通信用のプログラムを実行する前に、まず、定義ファイル 22 を最新のものに更新しておく機能を持つ。この発明では、メールソフトやブラウザやダイヤルアッププログラムなど、ネットワークに接続をして通信を実行するプログラムの起動時に、自動的にウィルス対策ソフトによる定義ファイルの修正分取り込み処理を実行させる。これによって、常に最新の定義ファイルを利用し、例えば、モバイルコンピュータがネットワークを通じて安全に通信をすることができる。

【0029】

図 2 は、ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。

この図を、図 1 と比較して説明する。コンピュータ 10 には、ウィルス対策プ

プログラム 16 の代りにパッチファイル取り込みプログラム 19 が設けられている。なお、1 台のコンピュータにウィルス対策プログラム 16 とパッチファイル取り込みプログラム 19 を合わせて備えることが好ましいが、説明の都合上それぞれ独立に実例を示した。ネット接続制御プログラム 17 は、ダイヤルアッププログラム 15 を起動した後に、パッチファイル取り込みプログラム 19 を起動するように動作する。ネットワーク 1 にはサーバ 25 が接続されている。このサーバ 25 は、メーラー（メール管理プログラム）13 やブラウザ 14 を提供する提供元が管理する。サーバ 25 に設けられた記憶装置 26 には、メーラー（メール管理プログラム）13 やブラウザ 14 のセキュリティ改善のためのパッチファイル 23 が記憶されている。パッチファイル取り込みプログラム 19 は、ネットワーク 1 を通じてパッチファイル 23 をダウンロードし記憶装置 12 に記憶する機能を持つ。このパッチファイル 23 によってメーラー（メール管理プログラム）13 やブラウザ 14 がその都度更新される。

【0030】

図 3 は、図 1 に示したプログラムの動作中表示される画面例の説明図である。

既に説明したように、例えば、メーラーの起動がされると、ダイヤルアッププログラム 15 の処理が開始されて、ネットワークの接続条件の設定が行われる。続いて、ウィルス対策プログラム 16 の定義ファイル修正分取り込みプログラム 18 が起動して、自動的に定義ファイルの修正分取り込み処理が実行される。このとき、その処理が完了したことをユーザに伝えるために、図 3（a）の画面 31 が表示される。ここでは、ユーザに対し、「ウィルス定義ファイルの更新をしました」というメッセージを表示し、その後安心してメーラー（メール管理プログラム）13 を利用できることをユーザに伝える。ユーザは、ボタン 41 をクリックしてこの画面 31 を閉じる。その後はメーラー（メール管理プログラム）13 が起動して通常通りメールの送受信が可能になる。なお、ブラウザは画面を表示すると既にネットワークを通じて初期画面のダウンロードを開始する。従って、ブラウザの画面表示より前に、定義ファイル 22 の更新処理やブラウザのパッチファイルを当てる処理を実行しておくことが好ましい。

【0031】

ウィルス定義ファイルの修正分取り込み処理は、既知の方法でよく、例えば、XML データベース形式でサーバからダウンロードして、アップデートすればよい。また、アプリケーションプログラムのセキュリティホール修復の目的で、アプリケーションプログラム供給元から配布される。パッチファイル 23 の取得とパッチを当てる処理についても、同様の手順で実行できる。図 3 (b) は後者の場合の、表示画面 32 の例である。また、定義ファイル 22 やパッチファイル 23 の更新処理を実行する前に、ユーザの了解をとる方法もある。この場合には、図 3 (c) に示す画面 33 のように、「インターネット接続前にウィルス定義ファイルの更新をします」といったメッセージを表示する。

【0032】

ボタン 43 をクリックするとユーザの了解が得られた状態になり、定義ファイル更新分取り込みプログラム 18 が起動する。パッチファイル取り込みプログラム 19 の起動についても同様の制御が可能である。このほかに、定義ファイル 22 やパッチファイル 23 の更新処理をユーザの制御により実行することもできる。図 3 の (d) に示す画面 34 のように、ネットワークの接続条件設定直後に、「メール送受信の開始前にセキュリティ対策ファイルの更新をして下さい」といったメッセージを表示する。この画面で、ボタン 44 をクリックすると定義ファイル 22 の更新処理が実行される。またボタン 45 をクリックするとパッチファイル 23 の更新処理が実行される。

【0033】

図 4 は、ネット接続制御プログラム 17 をインストールしたときの動作説明図である。

ネット接続制御プログラム 17 は、多数のコンピュータにインストールされて、その機種を選ばず動作するように、以下の機能を持つことが好ましい。図 4 (a) の画面 35 に示すように、初めに、インストールされるべきコンピュータの通信用ソフトを検索する。そして、制御対象になるソフトを決定する。画面 35 には、リストボックス 37 とボタン 46 ~ 50 が設けられている。インストール直後、リストボックス 37 にコンピュータ中の通信用ソフトのリストを表示する。ユーザがこの中から普段使用しているメーラーとブラウザを選択する。不要な

ものはボタン48をクリックして削除する。また、ほかにも通信用ソフトがある場合には、ボタン46を押して追加する。リストに表示させるにはボタン47をクリックすればよい。こうして、制御の対象となる通信用ソフトを決定すると、ボタン49をクリックする。ボタン50ですべての処理をキャンセルすることもできる。以上の準備処理によって図4の(b)に示すような起動画面を生成する。

【0034】

起動画面38は、上記のようなネットワークセキュリティの強化を図りながら、メールやインターネットを利用するための、新たなアプリケーションの画面である。この画面38には、例えば「ネットワーク接続ユーティリティ」といった表題が付けられている。ボタン51をクリックするとメーラーが起動する。ボタン52をクリックするとブラウザが起動する。制御プログラムは、図のような画面38を表示するフォームと、ボタン51と52のクリックイベントにより実行されるコマンドのリストが含まれる。そのコマンドの意味は、画面38の下側に示したとおりである。

【0035】

図5は、ネット接続制御プログラムの動作フローチャートである。

図5(a)は、ネット接続制御プログラム17の具体的な動作フローチャートである。まず、ステップS1で、通信用プログラムの起動指示を待つ。図4の(b)に示した画面38を使用して、ボタン51をクリックしメーラーを起動した場合には、ステップS1からステップS2へ進む。ステップS2では、制御シーケンスを起動する。制御シーケンスとは、ステップS3からステップS7の、一連の処理のことである。ステップS3で、ダイヤルアップ接続を起動する。そして、ステップS4で接続を確立させる。これでネットワークとの接続が可能になったから、ステップS5で、修正分取り込み処理を起動させて、定義ファイル22の修正分をダウンロードさせる。もちろん、同時に、パッチファイル23のダウンロードを実行させることもできる。その後、ステップS6で、処理完了メッセージを表示する。最後に、ステップS7で、通信用プログラムを起動して処理を終了する。

【0036】

図5（b）は、制御プログラムのオプションとして設けられたプログラムである。ネットワークに接続をして既に定義ファイル22やパッチファイル23の更新処理を済ませた後、いったん通信用プログラムも終了させることがある。この場合に、ネットワークの接続を継続していれば、定義ファイル修正分取り込みプログラム18やパッチファイル取り込みプログラム19はそのまま正常に動作している。従って、一定時間おきに定義ファイル22やパッチファイル23の更新処理が自動的に実行されている。その後再び通信用プログラムを起動したときに、改めて起動時に定義ファイル22やパッチファイル23の更新処理を実行する必要はない。さもないと、通信用プログラムの起動に時間がかかり操作性を悪くする。そこで、図のステップS21で、ネットワーク接続中かどうかを判断する。ネットワークに接続中であれば、ステップS22で、接続後に更新したかどうかを判断する。接続後に1回でも更新をした履歴が記録されていれば、ステップS23で、制御プログラムの起動を中止する。もちろん、いったんネットワークを切断してしまった場合には、制御プログラムを起動させる。

【0037】

図6は、ネット接続制御プログラムの別の動作フローチャートである。

図6（a）は、ネット接続制御プログラム17をインストールしたときの初期設定動作を示すフローチャートである。まず、ステップS31で、インストールを完了すると、ステップS32で、通信用プログラムの検索をする。そして、ステップS33で、通信用プログラムリストを生成する。ここで、その結果を表示し、ステップS34で、追加要求があれば、ステップS35でリストに対し通信用プログラムの追加処理を実行する。ステップS36で、削除要求があれば、ステップS37でリストの一部を削除処理する。最後に、ステップS38で、制御プログラムの生成をする。図6（b）は、ネット接続制御プログラム17の起動制御をユーザに任せる場合のプログラムフローチャートである。即ち、ステップS41で、通信用プログラムの起動指示があると、ステップS42で、制御プログラムの起動を要求する画面を表示する。いずれかのボタンがクリックされると、該当するプログラムが起動する。この処理は既に説明をしたとおりである。

【0038】

上記のようにして、ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、必ず、セキュリティ対策用ファイルの更新処理を起動させるようにしたので、例えば、長期間定義ファイルの更新をしないまま使用していたコンピュータを突然ネットワークに接続した場合でも、ウィルスの侵入から確実にコンピュータを防御できる。

【0039】

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウェアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばCD-ROMのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

【図面の簡単な説明】

【図1】 ネットワークセキュリティ強化システムの具体例を示すブロック図である。

【図2】 ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。

【図3】 図1に示したプログラムの動作中表示される画面例の説明図である。

【図4】 ネット接続制御プログラムをインストールしたときの動作説明図である。

【図5】 ネット接続制御プログラムの動作フローチャートである。

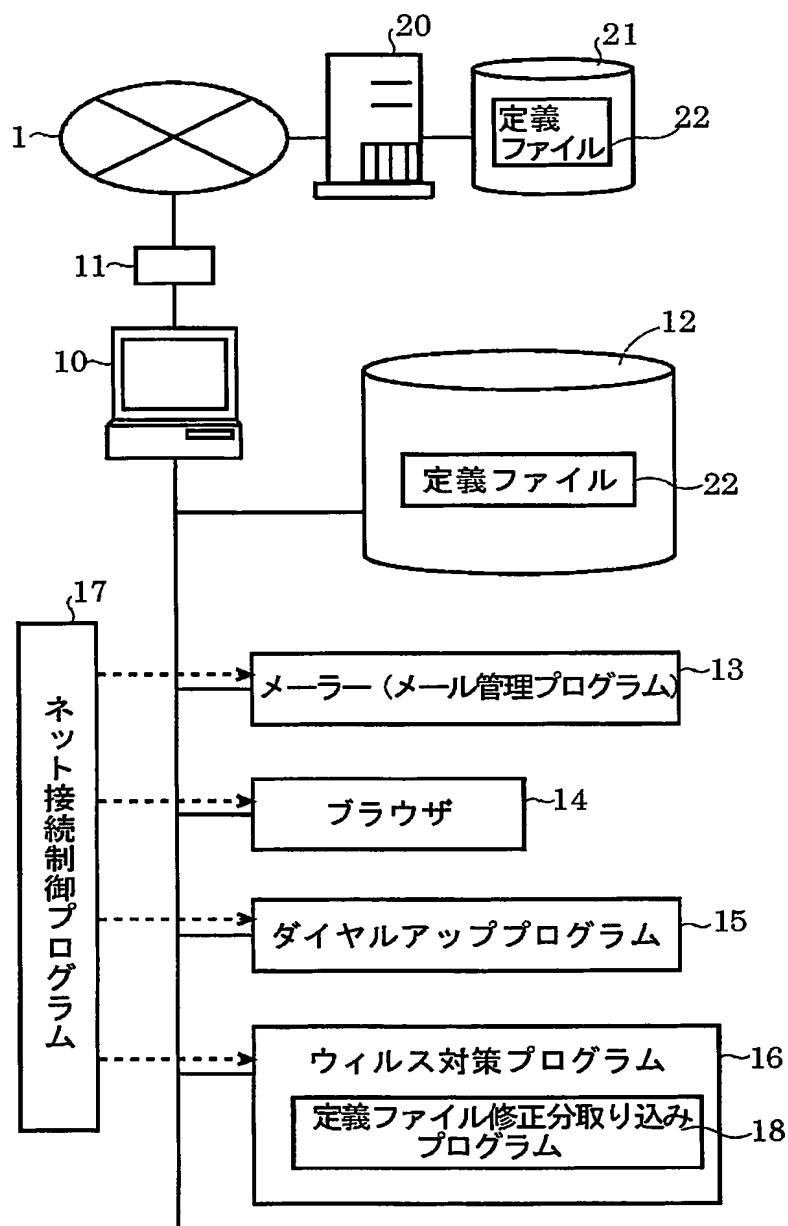
【図6】 ネット接続制御プログラムの別の動作フローチャートである。

【符号の説明】

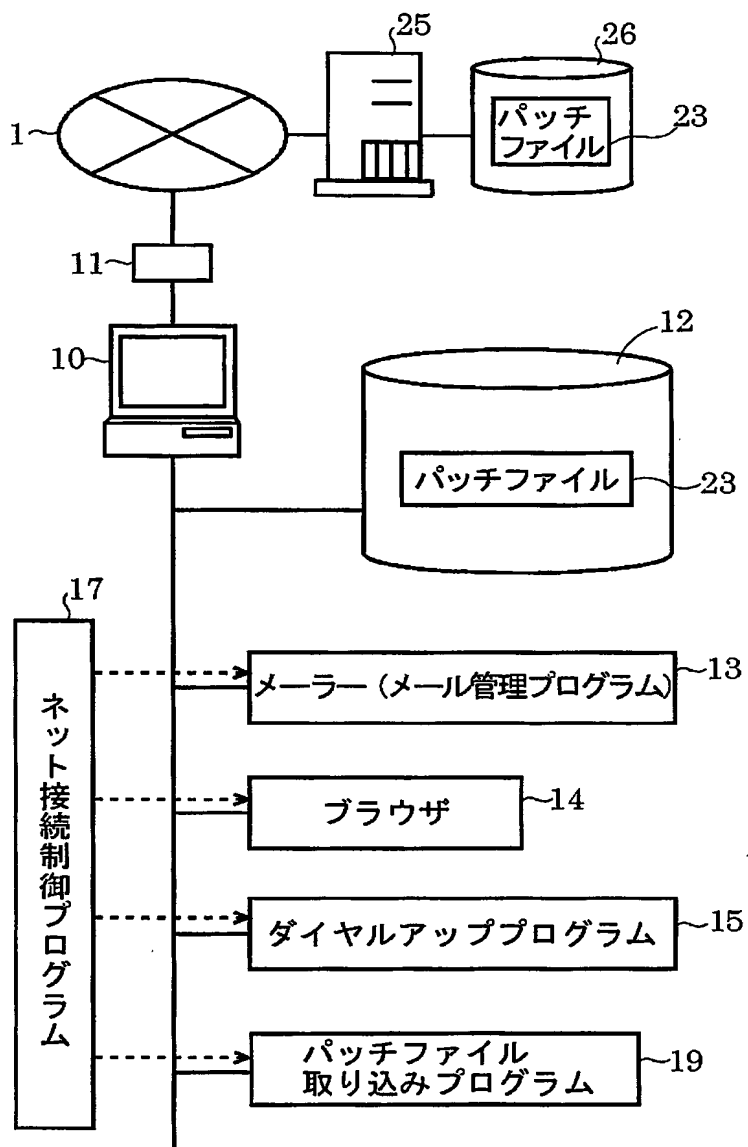
1 ネットワーク、 10 コンピュータ、 11 ネットワークインタフェース、 12 記憶装置、 13 メーラー（メール管理プログラム）、 14 ブラウザ、 15 ダイアルアッププログラム、 16 ウィルス対策プログラム、 17 ネット接続制御プログラム、 18 定義ファイル修正分取り込みプログラム、 19 パッチファイル取り込みプログラム、 20 サーバ、 21 記憶装置、 22 定義ファイル

【書類名】 図面

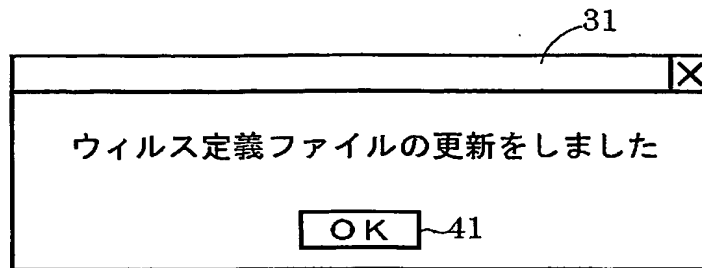
【図 1】



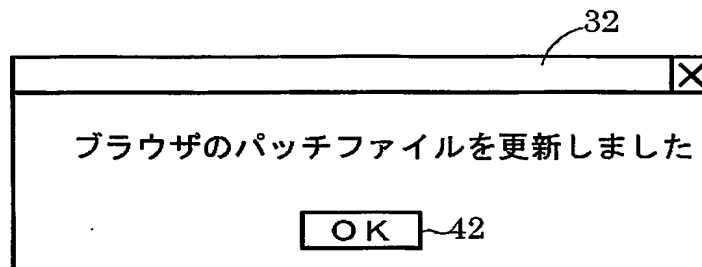
【図 2】



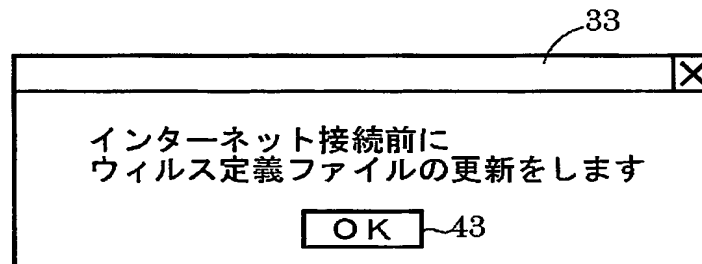
【図 3】



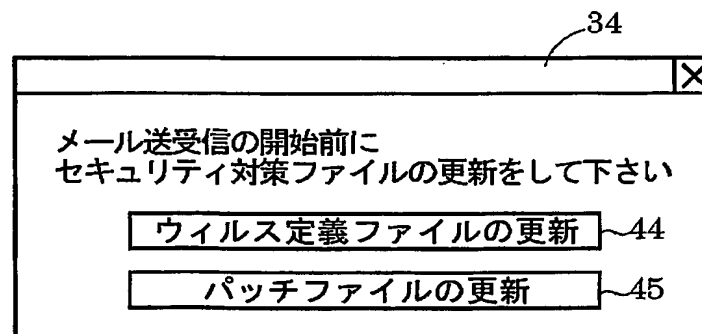
(a)



(b)

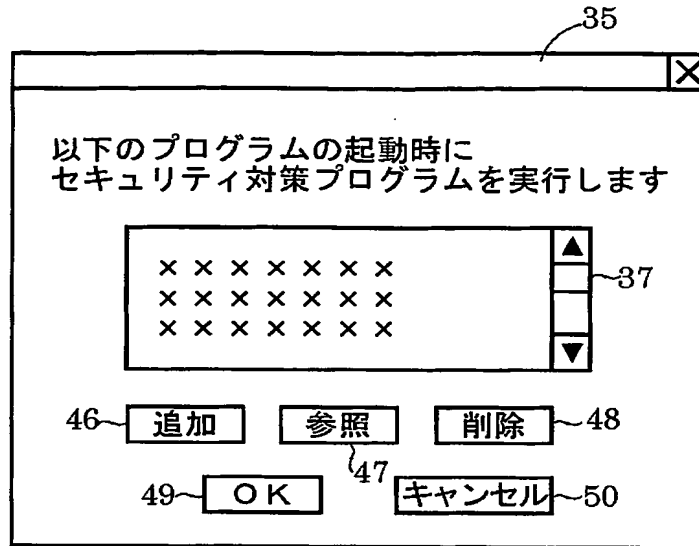


(c)

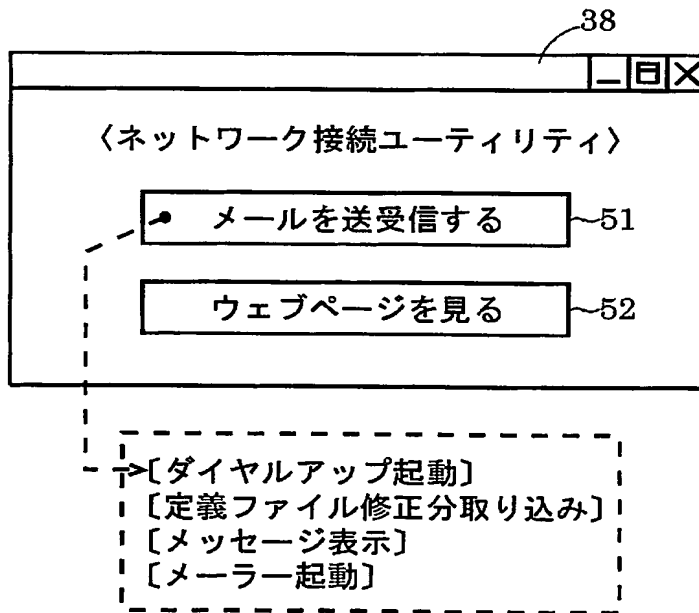


(d)

【図 4】

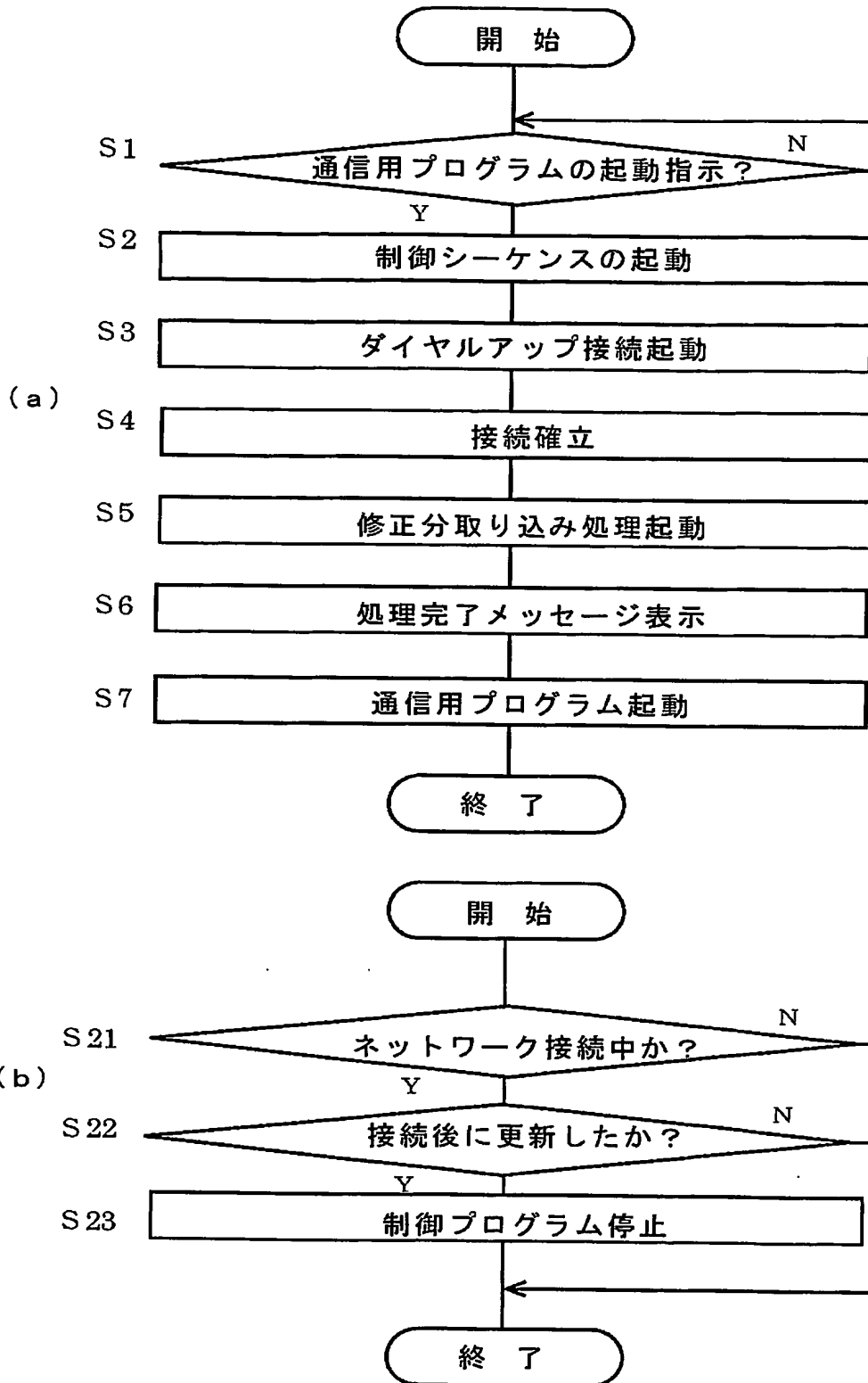


(a)

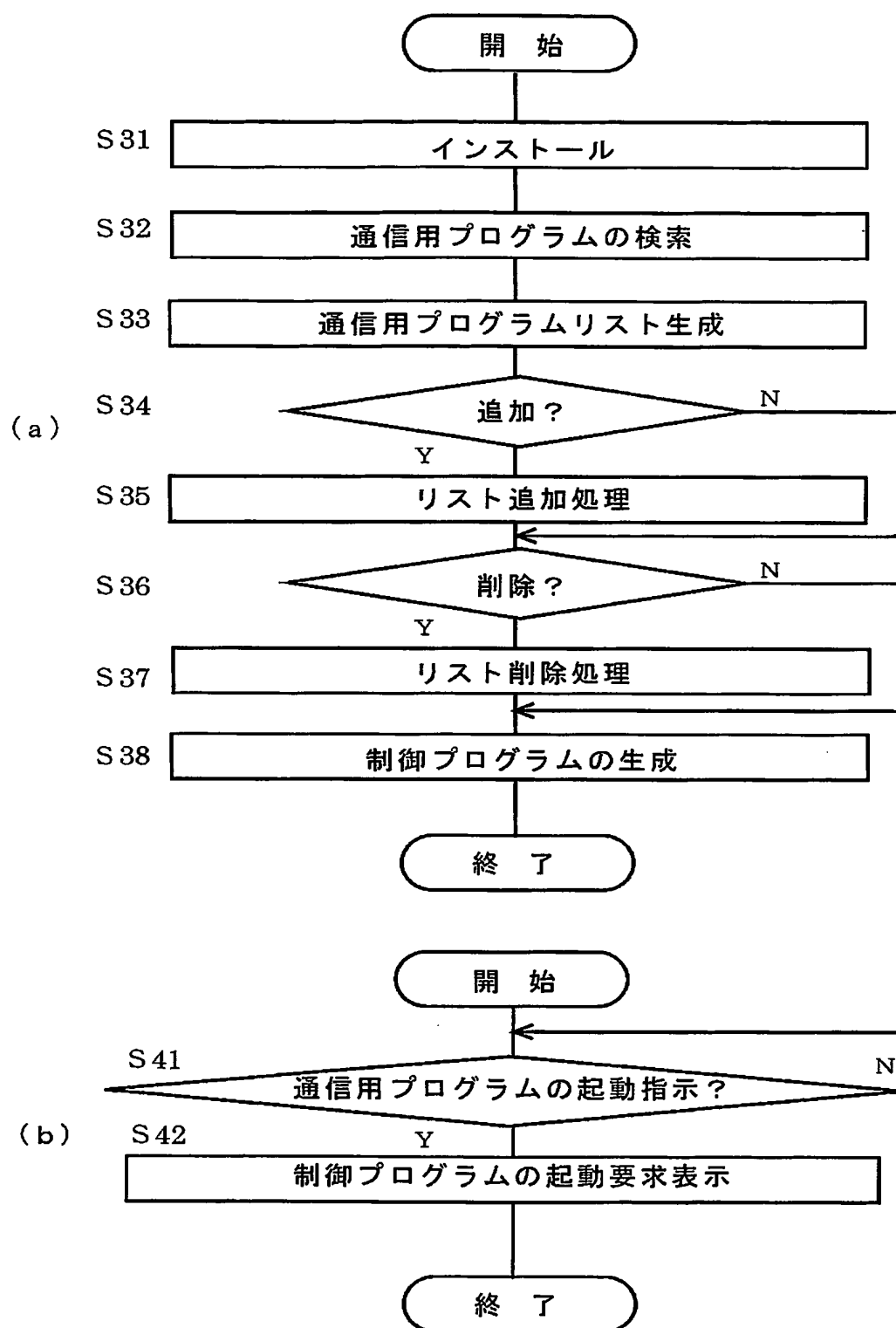


(b)

【図5】



【図 6】





【書類名】 要約書

【要約】

【課題】 常に最新のウィルス定義ファイルやパッチファイルを利用し、モバイルコンピュータがネットワークを通じて安全に通信ができるようにする。

【解決手段】 メールソフトやブラウザやダイヤルアッププログラムなど、ネットワークに接続をして通信を実行するプログラムの起動時に、自動的にウィルス対策ソフトを起動させる。そして、通信開始前に定義ファイルの修正分取り込み処理やパッチファイル更新処理を実行させる。さらに、セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 7 2 3 7 2
受付番号	5 0 3 0 0 4 3 3 9 6 9
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 3 月 1 8 日

<認定情報・付加情報>

【提出日】	平成15年 3月17日
-------	-------------

次頁無

特願 2 0 0 3 - 0 7 2 3 7 2

ページ : 1/E

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 3 6 9]

1. 変更年月日	1 9 9 0 年 8 月 2 0 日
[変更理由]	新規登録
住 所	東京都新宿区西新宿 2 丁目 4 番 1 号
氏 名	セイコーエプソン株式会社